ESERCIZI ESAME CYBER

Esercizi PDF prof

1) Let us consider a simple monoalphabetic shift cipher (Caesar's Cipher), with an alphabet of di N characters (with N= 26), with a secret key K=4 (the shift). Do encrypt the text "SECRET".

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

E(SECRET) ↝ "WIGVIX"

S+4 = W
E+4 = I
C+4 = G
R+4 = V
E+4 = I
T+4 = X

2) Consider a monoalphabetic substitution cipher, that maps a plaintext character *M* into the cipher character *C*, defined as follows:
$C = E_k(M) = a\,M + b \bmod 26$
where *M* is any character of the alphabet {'a','b', 'c', .. ,'z'}, and a and b are two integer parameters that form the secret key *K* = <a,b>
By using such a cipher, a ciphertext has been generated starting from an English plaintext. By analyzing the ciphertext it results that the most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Try to break this code, by knowing that the two most frequent letters in English are 'e' and 't'.
(Hints: x mod n = y ⇒ ∃ h : x = y +hn. The equation 15x mod 26 = 19 has the solution x = 3).

"approccio a tentativi"

PER CAPIRE L'INDIZIO ↝ $15x \bmod 26$ è il RESTO di $\frac{15x}{26}$ ↝

x=1 ↝ $15 \cdot 1 \bmod 26 = 15$ (perché 15:26 = 0 → resto 15)
x=2 ↝ $15 \cdot 2 \bmod 26 = 4$ (30:26 = 1, qualcosa con resto 4)
x=3 ↝ $15 \cdot 3 \bmod 26 = 19$ (45:26 = 1, qualcosa con resto 19) → risultato è x=3

$M_1 = 'e' = 4 \rightarrow C_1 = 'B' = 1$
$M_2 = 't' = 19 \rightarrow C_2 = 'U' = 20$
} informazioni della traccia dell'esercizio

- sostituzione nel cifrario

$(aM_1+b) \bmod 26 = C_1 \quad (4a+b) \bmod 26 = 1$
$(aM_2+b) \bmod 26 = C_2 \quad (19a+b) \bmod 26 = 20$

- RISOLVO SISTEMA PER SOSTITUZIONE: ricavo b dalla prima equazione e sostituisco nella prima

$(4a+b) \bmod 26 = 1 \rightsquigarrow b = 1-4a+h\cdot 26$ — derivo dalla DEF di sol. di un eq. modulare (VEDI HINT)

$(19a+b) \bmod 26 = 30 \rightsquigarrow (19a-4a+1+26h) \bmod 26 = 30$

$15a \bmod 26 = 29 \rightsquigarrow a = 3$ (* DA INDIZIO) $\rightsquigarrow$ sostituisco $\rightarrow b = 1-12+26 = 15$

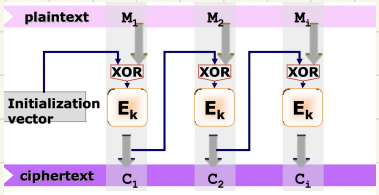
* per trovare risultato dell'equazione è possibile usare algoritmo di euclide

3) Starting from a block cipher $E_K()$ with block size q, please show the scheme for the CBC (Cipher Block Chaining) encryption of a message m with length $L>q$ (for simplicity, let's consider $L=n\,q$).

↳ in caso contrario si aggiunge padding

$m = M_1 || M_2 || \dots || M_n$
$c = C_1 || C_2 || \dots || C_n$

$C_0 = IV$
$C_i = E_K(M_i \oplus C_{i-1})$



4) Suppose to have an API implementing a block cipher E in CBC mode, with block size q. The same block cipher in CBC mode has been used to encrypt a message m with length pq using a key K of size n bits. Evaluate the complexity of a brute force attack against the secret key K, by supposing to know both the plaintext m and the ciphertext c. In each attempt, the entire message is processed. Indicate the complexity in terms of the number of block encryptions (using the function E), as function of n, p and q.

numero massimo di chiavi = 2^n

↳ x ogni operazione di encryption ci vogliono p-operazioni = $p \cdot 2^n$

5) Let us consider a symmetric block cipher $E_k(\cdot)$ with size 4 bit.
By supposing that, given a secret key K, the encryption table of $E_k(\cdot)$ corresponds to the table at the right side, do encrypt in CBC mode with IV=0000 the following plaintext message:

m= 1100 1010 0010 1101

plaintext	*cinhertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

↳ $C_i = E_K(M_i \text{ XOR } C_{i-1})$

$C_0 = IV = 0000$

$C_1 = E_K(1100 \text{ XOR } 0000) = E_K(1100) = 0101$

$C_2 = E_K(1010 \text{ XOR } 0101) = E_K(1111) = 0111$

$C_3 = E_K(0010 \text{ XOR } 0111) = E_K(0101) = 1111$

$C_4 = E_K(1101 \text{ XOR } 1111) = E_K(0010) = 1101$

} $C = 0101\ 0111\ 1111\ 1101$

6) Let us consider the following plaintext message:

m = 1100 0000 1100 0000

encrypted by means of the same symmetric encryption algorithm $E_k()$ with block size 4bit and secret key K of the previous exercise (same encryption/substitution table) in OFB mode with IV=0001, resulting the following ciphertext:

c = 1000 0010 0001 1001 (IV=0001)

Show how it is possible to modify the ciphertext c in such a way that by decrypting it you obtain the following plaintext:

m'= 1100 0000 1001 0000

plaintext	ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

OFB ↝ C = m Xor o

In OFB lo XOR non è fatto con il C_i precedente ⇒ posso cambiare direttamente il BLOCCO che mi interessa

$M_3 = 1100$ ↝ $C_3 = 0001$

$M'_3 = 1001$ ↝ $C'_3 = 0100$

↝ cambio i bit del ciphertext nella stessa posizione in cui cambio il plaintext

7) Let us consider a message $m=M1||M2||M3||M4$, and suppose to decrypt it by means of a block cipher $E_K()$ in CBC mode (the block size of $E_K()$ is equal to the size of the blocks Mi), with $iv=IV0$, obtaining the ciphertext $c= C1||C2||C3||C4$. If an attacker modifies the ciphertext by rearranging the component blocks obtaining the new ciphertext c'= $C1||C3||C2||C4$, which will be the corresponding plaintext message $m'=M'1||M'2||M'3||M'4$ obtained by "erroneously" decrypting the ciphertext c'? Show the blocks $M'i$ as function of Mj and Cj with $j=1..4$.

* Della traccia del problema
↳ $C'_2 = C_3$

Encryption in CBC ↝ $C_i = E_k(M_i \oplus C_{i-1})$

Decryption in CBC ↝ $M_i = D_K(C_i) \oplus C_{i-1}$

$M_i \oplus C_{i-1}$

↝ della teoria

$m' = M'_1 || M'_2 || M'_3 || M'_4$

$c' = C_1 || C_3 || C_2 || C_4$

↝ della traccia

$M'_1 = D_k(C'_1) \oplus IV = D_k(C_1) \oplus IV = (M_1 \oplus IV) \oplus IV = M_1$

$M'_2 = D_k(C'_2) \oplus C'_1 = D_k(C_3) \oplus C_1 = (M_3 \oplus C_2) \oplus C_1$

$M'_3 = D_k(C'_3) \oplus C'_2 = D_k(C_2) \oplus C_3 = (M_2 \oplus C_1) \oplus C_3$

$M'_4 = D_k(C'_4) \oplus C'_3 = D_k(C_4) \oplus C_2 = (M_4 \oplus C_3) \oplus C_2$

8) Realize a symmetric encryption scheme for encrypting messages *m* with any length, based on a block cipher $E_K()$ (e.g. AES), without obtaining avalanche effect, in such a way that if you change one bit of the ciphertext, only one bit of the plaintext will change when decrypting the ciphertext (hint: use the XOR operator).

→ da approfondire

↳ schema generale

PLAINTEXT $m = M_1 || M_2 || \dots || M_n$

ciphertext $c = IV || C_1 || C_2 || \dots || C_n$

$C_i = M_i \oplus O_i$

con $O_i = E_K(O_{i-1}) = AES(k, O_{i-1})$

$O_0 = IV$

9) Consider the following three padding algorithms for extending the length of a message to a multiple of N bytes (e.g. N=32). Which of the three algorithms are suitable for using with a block cipher with block size N bytes? Why?

Padding1: append to the message random bytes until the total length (in bytes) becomes a multiple of N.

Padding2: append to the message random bytes until the total length (in bytes) becomes a multiple on N – 1; append one byte encoding the number of padding bytes that have been added.

Padding3: append to the message a bit '1', then append as many bits '0' as needed to reach a multiple of N bytes.

1° ↝ BIT PADDING

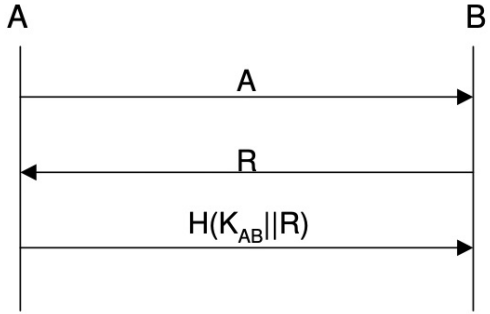
2° ↝ ANSI X.923

3° ↝

} ok per rendere messaggio divisibile in blocchi ma solo 2° e 3° vanno bene per encryption/decryption perché segnano quando inizia/finisce il padding

10) Starting from a hash function H() and a symmetric key K_{AB} shared between two entities A e B:
   i) show a possible authentication scheme between A (supplicant) and B (authenticator);
   ii) show how it is possible to send a message *m* from A to B providing data authentication and integrity protection;
   iii) create an encryption function (and the corresponding decryption function) that can be used for sending a message *m* encrypted from A to B.

i) A possible authentication scheme between A (supplicant) and B (authenticator):



(dalla teoria, CAPITOLO 2)

ii) Authentication and integrity protection of a message *m* sent from A to B:

11) Find the multiplicative inverse of each nonzero element in Z_7.

$Z_7 = \{1,2,3,4,5,6\}$

$1 \cdot x \equiv 1 \mod 7 \rightsquigarrow 1$
$2 \cdot x \equiv 1 \mod 7 \rightsquigarrow 4$ ($4 \cdot 2 = 8$, resto $= 1$ in $\mod 7$) ($8 \% 7 = 1$)
$3 \cdot x \equiv 1 \mod 7 \rightsquigarrow 5$ ($3 \cdot 5 = 15 \rightsquigarrow$ resto $= 1 \mod 7$) ($15 \% 7 = 1$)
$4 \cdot x = 1 \mod 7 \rightsquigarrow 2$ ($4 \cdot 2 = 8 \rightsquigarrow$ resto $= 1 \mod 7$)
$5 \cdot x = 1 \mod 7 \rightsquigarrow 3$
$6 \cdot x = 1 \mod 7 \rightsquigarrow 6$

↳ moltipli inversi $= 1,4,5,2,3,6$

12) Find all nonzero elements in Z_{21} that are relatively prime with 21.

Per trovare il numero degli elementi calcolo $\phi(21) = \phi(7 \times 3) = (3-1)(7-1) = 12$
↳ della teoria

↳ $U_{21} = \{1,2,4,5,8,10,11,12,13,16,17,19,20\}$

13) By using the Euclid's algorithm, find the greatest common divisor gcd(,) of:
a) 36, 15
b) 47, 20
c) 43, 35

GCD (36, 15)

$36 = 2 \cdot 15 + 6$

$15 = 2 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0$

↳ m.c.d

GCD (47, 20)

$47 = 2 \cdot 20 + 7$

$20 = 2 \cdot 7 + 6$

$7 = 1 \cdot 6 + 1$

$1 = 1 + 0$

↳ m.c.d

GCD (43, 35)

$43 = 1 \cdot 35 + 8$

$35 = 4 \cdot 8 + 3$

$8 = 2 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$1 = 1 + 0$

↳ m.c.d

14) Prove the following: If p and q are prime, then $\Phi(pq) = (p-1)(q-1)$.
(Hint: What numbers have a factor in common with pq?)

i numeri interi minori di pq sono $p, 2p, 3p \dots (q-1)p, q, 2q, 3q, (p-1)q$

$(q-1) + (p-1)$ valori totali

$\Phi(qp) = pq - [(q-1) + (p-1)] = qp - q - p + 1 = (p-1)(q-1)$

15) Create a pair of public/private RSA keys, using as p and q primes the values p=3, q=11. With such keys, do encrypt the plaintext message m=2.

$p=3, q=11$ e $m=2$

↳ $n = p \cdot q = 33$

↳ $\Phi(n) = 2 \cdot 10 = 20$

Per scegliere e: $[1,3,7,9,11,13,17,19]$ → scelgo 7

↳ calcolo d con algoritmo Euclideo esteso

k	q_k	r_k	x_k	y_k
0		20	1	0
1		7	0	1
2	$20 = 2 \cdot 7 + 6$	1	-2	
3	$7 = 1 \cdot 6 + 1$	-1	3	⇝ d=3
4	$6 = 6 \cdot 1 + 0$			

$K^+ = <e,n> = <7,33>$

$K^- = <d,n>$ (potrebbe anche essere $<p,q,n> = <3,33>$)

$c = E(m) = 2^7 \bmod 33 = 128 \bmod 33 = 29$

VERIFICO CORRETTEZZA CALCOLANDO $m \rightsquigarrow D(c) = 29^3 \bmod 33 = 2$ *

* TIP IMPORTANTE SE SI USA LA CALCOLATRICE

1) FARE $29^3 = 24389$

2) DIVIDERE PER MODULO ⇝ $\frac{24389}{33} = 739{,}0606061$

3) RIMUOVERE PARTE INTERA ⇝ $0{,}0606061$

4) MOLTIPLICARE X MODULO ⇝ $0{,}0606061 * 33 = 2$

16) With the following values p=7, q=11 and e=13. Create a pair of public/private RSA keys KU=<e,n> and KR=<d,n> (Use the Euclid's algorithm for finding the value d). With such keys, do decrypt the ciphertext message c=2.

1) calcolo $n = 7 \cdot 11 = 77$

2) calcolo $\phi(n) = 60$

3) calcolo d

k	r_k		x_k	y_k
0		60	1	0
1		13	0	1
2	$60 = 4 \cdot 13 + 8$		1	-4
3	$13 = 1 \cdot 8 + 5$		-1	5
4	$8 = 1 \cdot 5 + 3$		2	-9
5	$5 = 1 \cdot 3 + 2$		-3	14
6	$3 = 1 \cdot 2 + 1$		5	-23
7	$2 = 2 \cdot 1 + 0$			

$\rightsquigarrow d = -23 \bmod 60 = -23 + 60 = 37$

$m = D(c) = 2^{37} \bmod 77 = (2$

$37 =$

17) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

$m = D(C) = C^d \bmod n = 10^{(5)} \bmod 35 = 5$

$35 = 5 \cdot 7 \rightsquigarrow p = 5$ e $d = 7$

$\Phi(n) = 6 \cdot 6 = 24$

$d \rightsquigarrow$ uno degli interi ottenuti da Euclide

k	q_k	r_k	x_k	y_k
0		24	1	0
1		5	0	1
2	$24 = 4 \cdot 5 + 4$	1	-4	
3	$5 = 1 \cdot 4 + 1$	-1	5	$\rightsquigarrow d = 5$
4	$4 = 4 \cdot 1 + 0$			

↳ STOP

18) In an RSA system, the public key of a given user is $e = 31$, $n = 901$. What is the private key of this user? (*Hint:* First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find d)

$e = 31$

trovato iniziando a dividere 901 per tutti i numeri primi

$901 : 17 = 53 \rightsquigarrow p = 17$ e $q = 53$

$\Phi(n) = 832$

calcolo d

k	q_k	r_k	x_k	y_k
0		832	1	0
1		31	0	1
2	$832 = 26 \cdot 31 + 26$	1	-26	
3	$31 = 1 \cdot 26 + 5$	-1	25	
4	$26 = 5 \cdot 5 + 1$	6	-151	

risultato 681

$d = 681$ (convertito in mod 832)

Private Key = $\langle d, n \rangle = (681, 901)$

19) Show an example of shared key exchange between A and B based on Diffie-Hellman scheme, using the generator g=2 and the prime p=11.

A vuole $x_A = 5$ e B vuole $x_B = 3$

X LE FORMULE → VEDI 1.3

↳ A manda a B → $y_A = g^{x_A} \bmod p = 2^5 \bmod 11 = 32 \bmod 11 = 10$

B manda ad A → $y_B = g^{x_B} \bmod p = 2^3 \bmod 11 = 8 \bmod 11 = 8$

B calcola la sua chiave $K_{BA} = y_A^{x_B} \bmod p = 10^3 \bmod 11 = 10$

A calcola la sua chiave $K_{AB} = y_B^{x_A} \bmod p = 8^5 \bmod 11 = 10$

} sono uguali → OK

20) Show that 2 is a primitive root of 11.

calcolo le potenze da 0 a 10 di 2 in mod 11 →

$2^1 \bmod 11 = 2$
$2^2 \bmod 11 = 4$
$2^3 \bmod 11 = 8$
$2^4 \bmod 11 = 5$
$2^5 \bmod 11 = 10$
$2^6 \bmod 11 = 9$
$2^7 \bmod 11 = 7$
$2^8 \bmod 11 = 3$
$2^9 \bmod 11 = 6$
$2^{10} \bmod 11 = 1$

→ {1,2,3,4,5,6,7,8,9,10}

↳ sono tutti coprimi con 11 → 2 è primitive root con 11

21) Users A and B use the Diffie-Hellman key exchange technique with a common prime p=71 and a primitive root g=7.
i. If user A has private key x_A=5, what is A's public key y_A?
ii. If user B has private key x_B=12, what is B's public key y_B?
iii. What is the shared secret key K_{AB}?

p=71 g=7

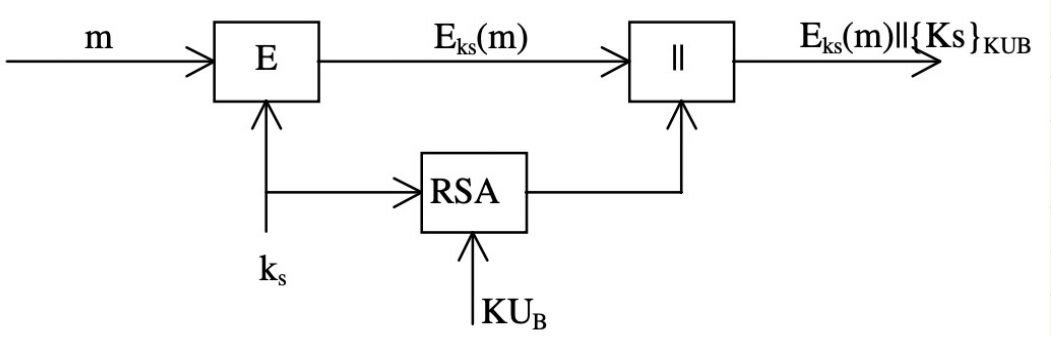
i) $y_A=5$, $y_A=?$ ↝ $y_A = g^{x_A} \bmod p = 7^5 \bmod 71 = 51$ (fatto con calcolatrice)

ii) $x_B=12$, $y_B=?$ ↝ $y_B = g^{x_B} \bmod p = 7^{12} \bmod 71 = 4$ (da imparare a calcolare!)

$7^{12} = 7^5 \cdot 7^7 \rightsquigarrow \left(7^5 \bmod 71 \cdot 7^7 \bmod 71\right) \bmod 71$
$(51 \cdot 16) \bmod 71 = 4$

iii) $K_{AB}=?$ ↝ $K_{AB} = y_B^{x_A} \bmod p = 4^5 \bmod 71 = 30$ (fatto con calcolatrice)

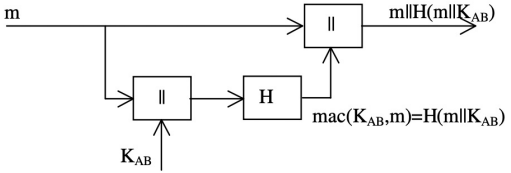
Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing ONLY the data confidentiality. For message encryption you should use a symmetric encryption algorithm (since it is faster than asymmetric algorithm). By supposing that A and B share only their public RSA keys KU_A e KU_B (KR_A and KR_B are the private keys), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes.



K_s è la SESSION KEY

23) Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing ONLY data authentication/integrity. By supposing that A and B share only a secret key K_{AB} and a hash algorithm H(), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes.

SOLUTION
Sender:

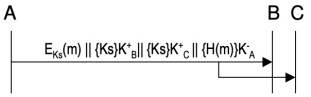


24) Let us suppose that you want to securely send a message *m* from A to B, by guaranteeing both confidentiality and data authentication/integrity. For message encryption you should use a symmetric encryption algorithm (since it is faster than asymmetric algorithm). By supposing that A and B share only their public RSA keys KU_A e KU_B (KR_A and KR_B are the private keys), show which functions can be executed at the sender and receiver sides. Try to depict the corresponding schemes. A and B share the following algorithms: RSA, AES, SHA1.

$X = AES_{k_s}(m) \,||\, RSA_{KU_b}(k_s) \,||\, RSA_{KR_A}(H(m))$ ⇝ non chiedermi perché 🤷🏽

25) Let us suppose that you want to securely send a message *m* from A to two recipients B and C, by guaranteeing both confidentiality (through symmetric encryption with algorithm $E_K()$) and data authentication/integrity (through digital signature). Let us suppose that A, B and C have their own private RSA keys, K^-_A, K^-_B e K^-_C , and that they share all their public keys K^+_A, K^+_B e K^+_C.
Please show which functions could be executed by A (sender), and the resulting message *x* that is actually sent from A to B and C.

SOLUTION
Sender:

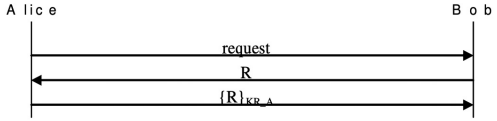


$X = E_{Ks}(m) \,||\, \{Ks\}K_B^+ \,||\, \{Ks\}K_C^+ \,||\, \{H(m)\}K_A^+$

↳ messaggio criptato OR chiave pubblica K_B insieme a K_S OR chiave pubblica K_C insieme a K_S OR $H(m)$ (hash) con chiave privata K_A^-

26) Show a possible secure authentication scheme between Alice (supplicant) and Bob (authenticator), by supposing that Alice and Bob share their public RSA keys KU_A and KU_B (KR_A and KR_B are the corresponding private keys).

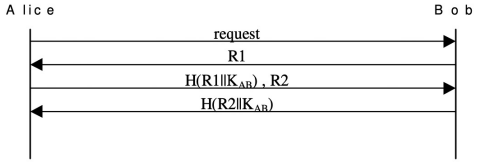
SOLUTION



↳ ci sono altre soluzioni possibili → non mi interessa!

27) Show a possible mutual authentication scheme between Alice and Bob, based on the use of an hash function H() and a shared secret K_{AB}.

SOLUTION



28) Show a possible key transport scheme between two entities A and B, based on asymmetric encryption (public key cryptography), without the use of a KDC.

$A \rightarrow B: \{K_s, sign_A(ID_B, K_s)\}_{KU_B}$

↳ possibile aggiungere un timestamp: $A \rightarrow B: \{K_s, t, sign_A(ID_B, K_s, t)\}_{KU_B}$

29) Show an example of authenticated DH exchange that holds out against MITM attack.

SOLUTION

An example of authenticated DH that uses only digital signature is:

$A \rightarrow B$: A, g^{Xa}

$A \leftarrow B$: B, g^{Xb}, $Sign_B(g^{Xa} \| g^{Xb} \| A)$

$A \rightarrow B$: $Sign_A(g^{Xa} \| g^{Xb} \| B)$

An authenticated DH that uses both signature and encryption is (it is a varian of the STS protocol):

$A \rightarrow B$: g^{Xa}

$A \leftarrow B$: g^{Xb}, $E_{Ks}(B \| Sign_B(g^{Xa} \| g^{Xb}))$

$A \rightarrow B$: $E_{Ks}(A \| Sign_A(g^{Xa} \| g^{Xb}))$

Where K_S is a key derived by the DH result g^{XaXb}.

} della teoria

30) Let us consider an entity A that holds the following digital certificates: $cert_{CA3}(A)$, $cert_{CA2}(CA3)$, $cert_{CA1}(CA2)$, and $cert_{CA1}(CA1)$ (where $cert_Y(X)$ refers to the certificate of X signed by Y). Indicate what A should send to B in order to let A and B start a secure communication, under the following different hypotheses:

B owns:	A should send to B:
$cert_{CA1}(CA1)$	$cert_{CA3}(A), cert_{CA2}(CA_3), cert_{CA1}(CA_2)$
$cert_{CA3}(A)$	nessun certificato
$cert_{CA1}(CA2)$	$cert_{CA3}(A), cert_{CA2}(CA_3)$
$cert_{CA1}(CA1)$, $cert_{CA3}(A)$	nessun certificato richiesto

31) If A holds $cert_B(A)$ and $cert_C(B)$ (where $cert_Y(X)$ refers to the certificate of X signed by Y), while D holds $cert_E(D)$, please indicate:
   a. what should A hold in order to authenticate D? Show a possible authentication scheme.
   b. what should D hold in order to authenticate A? Show a possible authentication scheme.

A: $cert_B(A)$, $cert_C(B)$

D: $cert_E(D)$

→

② A autentica D

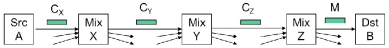
Per farlo A dovrebbe avere la chiave pubblica di E (visto che D possiede $cert_E(D)$)

D → A richiesta
A → D R ~ challenge - response
D → A: $\{R\}_{KR_D}$, $cert_E(D)$

⑥ D dovrebbe possedere la chiave pubblica di C:

A → D: request
D → A: R
A → D: $\{R\}_{KR_B}$, $cert_B(A)$, $cert_C(B)$

32) Let us consider an anonymizing network formed by high-latency anonymizing *Mix* nodes. Let us consider the case in which a node *A* wants to send a message *m* to a node *B* by means of three intermediate *Mix* nodes *X*, *Y*, and *Z*. Assume that K^+_i and K^-_i are respectively the public and private keys of node *i* (*i*=*x*,*y*,*z*).
Indicate the format of the message C_X composed by *A* and sent to the first node *X*.



$$C_X = E_{K_X}(ID_Y \| E_{K^+_Y}(ID_Z \| E_{K^+_Z}(ID_B \| m)))$$

$$C_Y = E_{K^+_Y}(ID_Z \| E_{K_Z}(ID_B \| (m)))$$

$$C_Z = E_{K^+_Z}(ID_B \| (m))$$

↝ in ogni passo nell'anello viene rimosso uno strato d'encryption.

33) Consider the following C function for verifying a user-provided password. Which type of attack it could be vulnerable to? What is a possible input password that could exploit such vulnerability?

```
int verifyPassword(char* pwd) {
      char str1[8];
      char str2[8];
      strcpy(str1,"SECRET"); // correct password is "SECRET"
      strcpy(str2,pwd);
      if (strncmp(str1,str2,8)==0) return 1; // compares the first 8 characters
      else return 0;
}
```

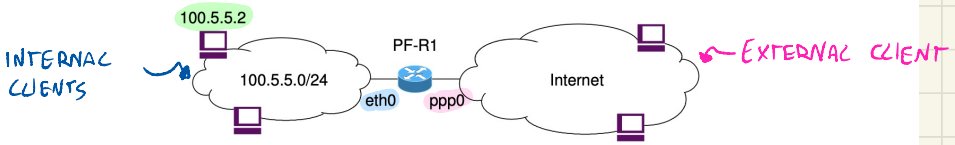
↳ BUFFER OVERFLOW ATTACK: se uso una password degli stessi 8 caratteri saranno uguali anche str2
nel caso la password fosse troppo lunga verrebbe danneggiato lo stack frame → DoS Attack

34) Let us consider the following network scheme, where in the node 100.5.5.2 there is a HTTP web server (TCP port 80) and a SMTP mail server (TCP port 25); you are requested to configure the filtering table of the router R1 so that:

i) from external clients it is possible to access to the internal web server (node 100.5.5.2, TCP port 80);

ii) from internal clients it is possible to access any external web server (port 80);

iii) all client/server and server/client communications between the internal SMTP mail server and possible external SMTP servers are enabled; that is, internal SMTP Client → external SMTP Server (TCP port 25), and external SMTP Client → internal SMTP Server (TCP port 25).



bisogna lavorare per punti

HP: tutte le connessioni predefinite devono essere accettate SEMPRE

	MATCHING								ACTION
	in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	state	ACCEPT/DROP
	*	*	*	*	*	*	*	ESTABLISHED	ACCEPT
i	ppo	eth0	*	100.5.5.2	TCP	*	80	NEW	ACCEPT
ii	eth0	ppo	* 100.5.5.0/24	*	TCP	*	80	NEW	ACCEPT
iii	ppo	eth0	*	*	TCP	*	25	NEW	ACCEPT
iii	eth0	ppo	100.5.5.2	*	TCP	*	25	NEW	ACCEPT
iv	*	*	*	*	*	*	*	NEW	DROP

* indirizzi che vanno da 0 a 24

IMPLICITO: droppare le altre connessioni

N.B. → se avessi avuto una regola per applicare ANTI-SPOOFING → aggiungere riga alla tabella in cui vengono DROPPATE tutte le connessioni

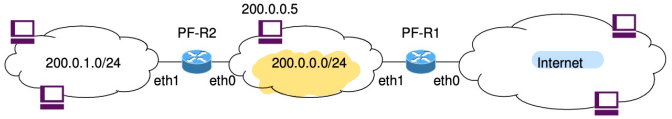
35) Let us consider the following company network formed by an internal network and a DMZ separated by a screening router R2, and connected to the external public network (Internet) through the screening router R1, as shown in figure.
You are requested to configure the filtering table of R1 so that:

a) it is possible to establish application level client→server communications (through any transport protocol) from any DMZ node to any external node;

b) it is blocked any attempt to establish a client→server communication from the external network to the DMZ;

c) it is blocked any communication between the internal and the external networks;

d) it is possible to establish TCP connections from the external network to the node 200.0.0.5 TCP port 80 (HTTP).



MATCHING | ACTION

	in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	state	ACCEPT/DROP
	*	*	*	*	*	*	*	ESTABLISHED	ACCEPT
a)	eth0	eth1	200.0.0.0/24	*	*	*	*	NEW	ACCEPT
d)	eth1	eth0	*	200.0.0.5	TCP	*	80	NEW	ACCEPT
b,c	*	*	*	*	*	*	*	NEW	DROP

ESERCIZI ESAMI VECCHI

11/06/2020

9) **Let us consider an block cipher $E_k(\cdot)$ used for encrypt a message $m=M_1||M_2||M_3||\ ..\ ||M_i||M_{i+1}||..$ using the CBC (Cipher Block Chaining) mode, please indicate the first and the generic i-th steps.**

C0 = ?
Ci = ?

Per CBC → $C_0 = IV$

$C_i = E_k(M_i \oplus C_{i-1})$

By supposing that, given a key K, the encoding function $E_k(\cdot)$ corresponds to the table at side, please encrypt the following message m in CBC mode, with IV=0000

m = 1101 1100 1010 0010

c = ?

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

$C_0 = IV = 0000$

$C_1 = E_K(M_1 \oplus C_0) = E_K(1101 \oplus 0000) = E_K(1101) = 1001$

$C_2 = E_K(M_2 \oplus C_1) = E_K(1100 \oplus 1001) = E_K(0101) = 1111$

$C_3 = E_K(M_3 \oplus C_2) = E_K(1010 \oplus 1111) = E_K(0101) = 1111$

$C_4 = E_K(0010 \oplus 1111) = E_K(1101) = 1001$

↓

$C = 1001\ 1111\ 1111\ 1001$

10) We want to create a RSA key pair $K^+=<e,n>$, $K^-=<d,n>$, starting from the two secret prime numbers p=3, q=17, and value e=25. For obtaining the value d of the private key, you can either use the Euclid's algorithm or try and test knowing that d is one of the following values: 3,5,7,9,11,13.
By using the private key K^- do decrypt the ciphertext c=4

$p,q=3,17 \rightsquigarrow n=3\cdot 17=51$

$\Phi(n)=2\cdot 16=32$

$e=25$

Per d uno teorema d'Euclide esteso ↝

$d=5$

$K^+=<25,51>$ $K^-=<9,51>$

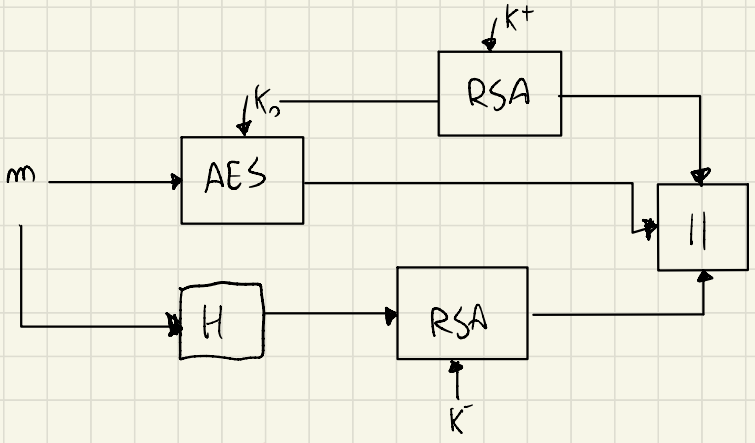
q_k	r_k	x_k	y_k
	32	1	0
	25	0	1
$32=1\cdot 25+7$		1	-1
$25=3\cdot 7+4$		-3	6
$7=1\cdot 4+3$		4	-5
$4=1\cdot 3+1$		-7	9 ↝ d=9
↳ stop			

$m=c^d \bmod n=4^9 \bmod 51=2^{18} \bmod 51=(2^5 \bmod 51 \cdot 2^{13} \bmod 51) \bmod 51=(32\cdot 32) \bmod 51=4$

$c=4^{25} \bmod 51=(4^5 \bmod 51 \cdot 4^{13} \bmod 51 \cdot 4^7 \bmod 51) \bmod 51$

$(4\cdot 4\cdot 13) \bmod 51=4$

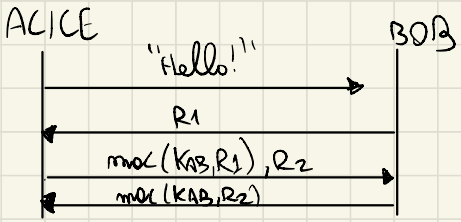
11) We want to store a large message *m* (e.g. a file) onto an insecure public storage system, by guaranteeing both the confidentiality and the integrity/authenticity of the data *m*. Let's suppose to have a RSA key pair $\{K^-, K^+\}$, and to have the following cryptographic algorithms: RSA, AES, SHA1. Please indicate a possible functional scheme that can be used for such a purpose, and the resulting data that will be actually stored.
(Note: if possible, use symmetric encryption for confidentiality)



$x = AES_{K}(m) \,||\, RSA_{K^+}(K) \,||\, RSA_{K^-}(H(m))$

non ne sono sicuro!

12) Show a possible challenge-response authentication scheme that can be used by Alice to authenticate Bob, based on a MAC function and a shared secret K_{AB}.



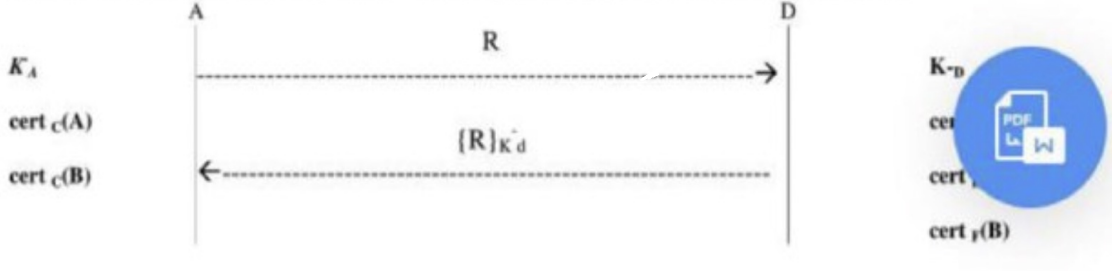
13) Show a possible message exchange for creating a group key among 3 participants (group members) using a Group Diffie-Hellman key exchange.

Tutti i partecipanti aderiscono ad un numero primo p ed un generatore g. Ogni partecipante genera un valore segreto x_i;
La KEY finale = $g^{x_1x_2x_3} \bmod p$
Per calcolarla ogni partecipante deve ricevere $y = g^{abc} \bmod p$ ed usare x_i per calcolare $y^{x_i} \bmod p = g^{abcx_i} \bmod p = g^{x_1x_2x_3} \bmod p$

↳ $U_1 \rightarrow U_2$: g^{x_1}
$U_2 \rightarrow U_3$: $g^{x_1x_2}, g^{x_2}$

$U_3 \rightarrow U_2$: $g^{x_1x_2x_3}, g^{x_3}$
$U_2 \rightarrow U_1$: $g^{x_2x_3}$

14) Let's consider the authentication scheme in figure where *A* wants to authenticate *D*. Consider that *R* is a random value and K^-_D is the private key of *D*). A has her own private key K^-_A, $cert_C(A)$ and $cert_C(B)$ (where $cert_Y(X)$ is a certificate of (owned by) *X* signed/issued by *Y*), while *D* has his own private key K^-_D, $cert_E(D)$, $cert_B(E)$, $cert_F(B)$. Which information should *A* and/or *D* add to message exchange in order to let *A* authenticate *D*?



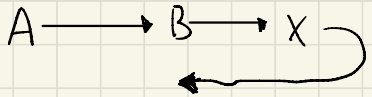
A: mando $cert_C(A)$.

D: mando $cert_E(D)$, $cert_B(E)$

A prendo da qui chiave di E (conoscendo B) per ottenere D

15) The entity A wants to anonymize a message *m* to be sent to B, by using a high-latency anonymizing *Mix* node X. Assume that K^+_i and K^-_i are respectively the public and private keys of node *i* (*i*=*A*,*B*,*X*).
What is a possible message that A will send to X for such a purpose?

$$x = E_{K^+_A}(ID_B \| E_{K^+_B}(ID_X \| E_{K^+_X}(ID_B \| m)))$$



Esame 23/06/2023

9) Given a symmetric block cipher $E_K()$, please show the first step and the generic *i*-step of the enciphering of a plaintext *m* using OFB (Output Feedback) mode. With $m=M_1\|M_2\|M_3\| \ldots \|M_{n-1}\|L$.

C0 = ?
Ci = ?

$C_0 = IV$

$C_i = M_i \text{ XOR } O_i$ con $O_i = E_K(O_{i-1})$ (one time pad)

10) Suppose to use a block cipher with block size 4 bit. Using a given key *K* the $E_K()$ function encrypts input (plaintext) blocks according to the table on the right.

Do encrypt the following plaintext *m* using OFP mode with IV=0001

m = 1100 0101 1100 0000

c= ?

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000

IV=0001

$C_1 = 1100 \oplus E_K(0001) = 1100 \oplus 0100 = 1000$

$C_2 = 0101 \oplus E_K(0100) = 0101 \oplus 0010 = 0111$

$C_3 = 1100 \oplus E_K(0010) = 1100 \oplus 1101 = 0001$

$C_4 = 0000 \oplus E_K(1101) = 0000 \oplus 1001 = 1001$

$C = 1000\ 0111\ 0001\ 1001$

11) Create a pair of RSA public/private key pair $K^+=<e,n>$ (public) and $K^-=<d,n>$ (private), starting from the two secret prime numbers p=5, q=11, and value d=23. For obtaining the value e of the public key, you can either use the Euclid's algorithm or try and test knowing that d is lesser than 20.
By using the public key K^+ do encrypt the plaintext m=4.

$p=5 \quad q=11$

↳ $n=55$; $\phi(n)=40$

$d=23$

n lo calcolo con teorema di Eulero

r_k	x_k	y_k	
40	1	0	
23	0	1	
$40=1\cdot 23+17$	1	-1	
$23=1\cdot 17+6$	-1	2	
$17=2\cdot 6+5$	+3	-5	
$6=1\cdot 5+1$	-4	7	⇝ e=7

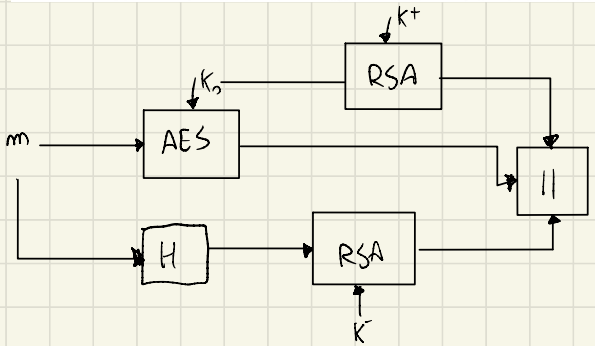
$c = m^e \bmod n = 4^7 \bmod 55 = 49$

$m = c^d \bmod n = 49^{23} \bmod 55 = (49^7 \bmod 55 \cdot 49^5 \bmod 55 \cdot 49^{11} \bmod 55) \bmod 55$

↳ $(49^5 \bmod 55 \cdot 49^2 \bmod 55 \cdot 49^2 \bmod 55 \cdot 49^3 \bmod 55 \cdot 49^5 \bmod 55 \cdot 49^3 \bmod 55 \cdot 49^3 \bmod 55) \bmod 55$

$(21 \cdot 36 \cdot 36 \cdot 4 \cdot 4 \cdot 21 \cdot 4) \bmod 55 = 4$ ok

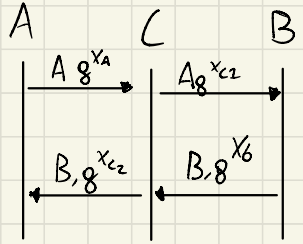
12) We want to store a large message *m* (e.g. a file) onto an insecure public storage system, by guaranteeing both the confidentiality and the integrity/authenticity of the data *m*. Let's suppose to have a private/public key pair K^- and K^+, and to have the following cryptographic algorithms: RSA, AES, SHA1. Please indicate a possible functional scheme that can be used for such a purpose, and the resulting data that will be actually stored.
(Note: if possible, use symmetric encryption for providing confidentiality)



$x = AES_{K_1}(m) \,||\, RSA_{K^+}(K_1) \,||\, RSA_{K^-}(H(m))$

Aes per confidenzialità
MAC per integrità del messaggio
RSA per autenticazione

13) Show an example of successful Man-in-the-middle attack against basic Diffie-Hellman exchange between two entities A and B.



C ottiene così le chiavi $K_1 = 8^{X_b X_{C2}}$ e $K_2 = 8^{X_A X_{C_2}}$

14) An entity A has her private key K_A^-, her certificate $cert_{CA3}(A)$ (that is the certificate of A signed/issued by CA3), and the following additional certificates: $cert_{CA2}(CA3)$, $cert_{CA1}(CA2)$, $cert_{CA0}(CA1)$, and $cert_{CA0}(CA0)$.
An entity B has his private key K_B^-, his certificate $cert_{CA5}(B)$, and the following certificates: $cert_{CA4}(CA5)$, $cert_{CA1}(CA4)$, $cert_{CA0}(CA1)$, and $cert_{CA0}(CA0)$
Which is the minimum set of certificates that A must send to B in order to let B authenticate A using a challenge/response scheme based on public key cryptography (e.g. using the A's signature)?

A

$cert_{CA_3}(A)$
$cert_{CA_2}(CA_3)$
$cert_{CA_1}(CA_2)$
$cert_{CA_0}(CA_1)$
$cert_{CA_0}(CA_0)$

B

$cert_{CA_5}(B)$
$cert_{CA_4}(CA_5)$
$cert_{CA_1}(CA_4)$
$cert_{CA_0}(CA_1)$
$cert_{CA_0}(CA_0)$

$A \rightarrow B$: $cert_{CA_3}(A)$, $cert_{CA_2}(CA_3)$, $cert_{CA_1}(CA_2)$ → STOP perché B conosce CA_1

$B \rightarrow A$: $cert_{CA_5}(B)$, $cert_{CA_4}(CA_5)$, $cert_{CA_1}(CA_4)$ → STOP perché A conosce CA_1

15) The entity A wants to anonymously send a message m to B, by using a sequence of two high-latency anonymity nodes (Mix nodes) P and Q. Assuming that for each entity X (with X=A,P,Q,B), K^+_x and K^-_x are the public and private keys, what is the message that A sends to P?

↳ $X = E_{K_A^+}(ID_P \,||\, E_{K_P^+}(ID_Q \,||\, E_{K_Q^+}(ID_B \,||\, E_{K_B^+}(ID_Q \,||\, m))))$

10) **Create a pair of RSA key pair K^+=<e,n> (public) and K^-=<d,n> (private), starting from the two secret prime numbers p=5, q=13, and public exponent *e*=11. For obtaining the value *d* of the private key, you can either use the Euclid's algorithm or try and test knowing that *d* is greater than 30.**
By using the private key K^- do decrypt the ciphertext *c*=2.

$n = p \cdot q = 5 \cdot 13 = 65$

$\phi(n) = 4 \cdot 12 = 48$

$e = 11$, per calcolare d uso teorema di Euclide esteso

	x_k	y_k
48	1	0
11	0	1
$48 = 4 \cdot 11 + 4$	1	-4
$11 = 2 \cdot 4 + 3$	-2	9
$4 = 1 \cdot 3 + 1$	7	-13

$\rightsquigarrow -13 \bmod 48 = 35$

$K^+ = \langle 11, 65 \rangle$ $K^- = \langle 35, 65 \rangle$

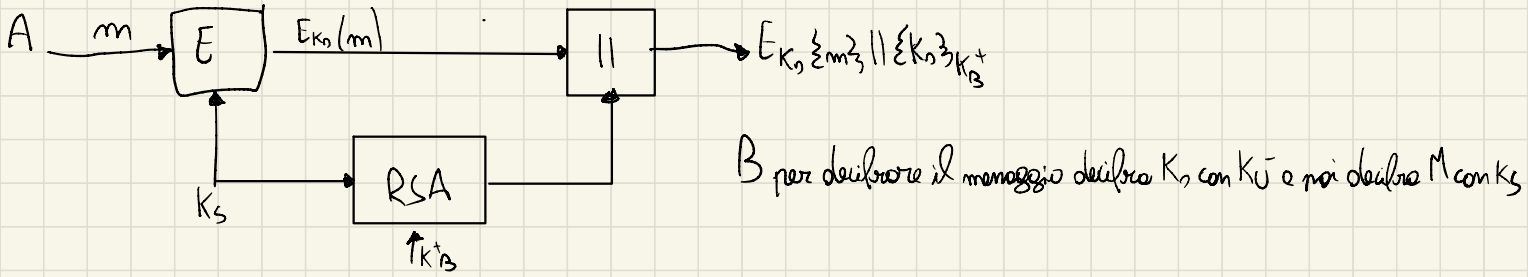
$m = c^d \bmod n = 2^{35} \bmod 65 = (2^{17} \bmod 65 \cdot 2^{18} \bmod 65) \bmod 65$

$\hookrightarrow (2^{17} \bmod 65 \cdot 2^2 \bmod 65 \cdot 2^3 \bmod 65 \cdot 2^5 \bmod 65 \cdot 2^7 \bmod 65 \cdot 2^5 \bmod 65 \cdot 2 \bmod 65) \bmod 65$

$(33 \cdot 4 \cdot 8 \cdot 32 \cdot 63 \cdot 32 \cdot 2) \bmod 65 = 49$

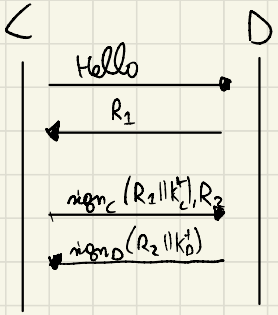
$c = 4^{11} \bmod 65 = 49 \rightarrow OK$

11) **An entity A wants to send a message *m* to B, by guaranteeing ONLY the confidentiality of the data (i.e. the message *m*). For the encryption of *m* A uses a symmetric encryption algorithm. If A and B do not share in advance any symmetric key, if both A and B have an own RSA private key (respectively K_A^- and K_B^-), and if they share the corresponding public keys K_A^+ and K_B^+, please indicate a possible scheme used by A to send the message and the scheme used by B to receive it:**



B per decifrare il messaggio decifra K_0 con K_U^- e poi decifra M con K_S

12) **Show a possible challenge-response authentication scheme that can be used by Carol to authenticate David, based on a digital signature algorithm using the private/public keys of Carol and/or David.**

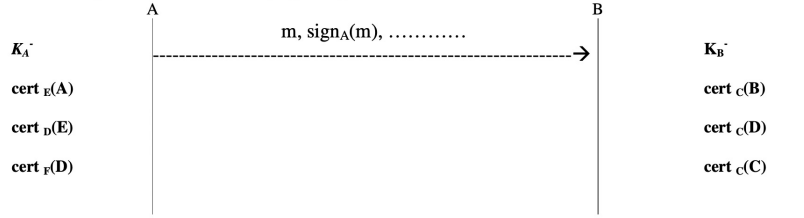


13) **Show an example of authenticated Diffie-Hellman exchange between Carol (C) and David (D) that resists against MITM attack from a possible third party intruder.**

$A \rightarrow B : A, g^{X_A}$

$A \leftarrow B : B, g^{X_B}, \text{sign}_B$

14) **An entity *A* wants to send a message *m* to *B* signed with her private key K_A^-. Consider that *A* has her own private key K_A^-, the $cert_E(A)$, $cert_D(E)$, and $cert_F(D)$, while *B* has $cert_C(B)$, $cert_C(D)$, and $cert_C(C)$. Which information should *A* add to message in order to let *B* verifying the signature?**



15) The entity A wants to anonymize a message m to be sent to D, by using the cascade of high-latency anonymizing *Mix* nodes B and C, in such a way that A→B→C→D is the sequence of nodes that will be involved in the delivery. Assume that K^{+}_{i} and K^{-}_{i} are the public and private keys of node i (with $i=A,B,C,D$). What is a possible message that A will send to B for such a purpose?